

WHAT IS CLAIMED IS:

Sub
al

1. A cryptographic system in a computer system, the cryptographic system comprising:

a central server;

a remote server;

a database on the central server responsive to signals from the central server, the database being configured to contain sensitive information;

enterprise credentials stored in the database;

a key repository process on the central server, the key repository process having one or more master keys for managing information in the database, the key repository process further configured to access the enterprise credentials and to authenticate authorizations to access the sensitive information in the database;

an agent on the remote server, the agent acting on behalf of the key repository process on the central server; and

at least one application on the remote server;

wherein the agent authenticates authorizations of specific applications to access resources based upon authorizations held and maintained by the key repository process on the central server.

2. A cryptographic system as in claim 1, wherein the key repository process and the agent communicate with each other, the communication being authenticated by a shared secret, and wherein the shared secret is protected by a level of trust equivalent to that with which the shared secret is protected on the central server by the key repository process.

3. A cryptographic system as in claim 2, wherein the level of trust is defined as the number of individuals required for reconstructing the master key and/or for performing a sensitive operation.

4. A cryptographic system as in claim 1, wherein the agent in the remote server is an independent key repository process with a level of trust equivalent to that of the key repository process in the central server.

5. The cryptographic system of claim 1, wherein at least one master key protects the sensitive information in the database.

6. The cryptographic system of claim 1, wherein at least one master key provides privacy protection to the sensitive information.

7. A method used in a cryptographic system for obtaining sensitive information, comprising:

storing enterprise credentials in a database on a central server, the database being configured to contain sensitive information;

establishing one or more master keys for managing information in the database by a key repository process, the key repository process being configured to access the enterprise credentials;

authenticating, by the key repository process, authorizations to access the sensitive information in the database;

establishing communications between the key repository process on the central server and an agent on a remote server, the agent acting on behalf of the key repository process on the central server; and

authenticating, by the agent, authorizations of specific applications on the remote server to access resources based upon authorizations held and maintained by the key repository process on the central server.

8. A method for obtaining cryptographic credentials by an application running on a computer system, comprising:

providing a computer system having at least one server and a cryptographically protected database;

5 instantiating a key repository process on the computer system, the key repository process being configured with a remote agent interface and/or for interface via a trusted link;

instantiating an application process on the computer system;

conducting, by the application process, a query of the key repository process for sensitive information, the query being conducted via the remote agent interface or the trusted

10 link if the application process and the key repository process are located on different servers; and

providing to the application process, by the key repository process, an encrypted file of the sensitive information, the encrypted file being provided via the remote agent interface or the trusted link if the application process and the key repository process are located on different servers.